

RESILIENCE BOARD

Executive summary

1. At its meeting on 27 September, Leadership Group (LG) considered a proposal to establish a Resilience Board to take strategic oversight of personnel, physical and cyber security as well as business continuity planning. The relevant paper is attached as Annex A. LG requested further information in two areas and this paper addresses that request.

Issues and Options

BCM Structure

2. No changes are proposed to the Business Continuity Management (BCM) structure below the strategic level. This means that the roles, remit and membership of the various teams (such as IMT, ICT BCT, IWT etc.) remain as they are. The Resilience Board will take responsibility for strategic direction and support to the Business Continuity Manager. This is in line with many major organisations which embed BC with other strategic response structures. Responsibilities for the management of High Impact Risks will also remain unchanged and risk owners will be expected to report to the Resilience Board on the maintenance and improvement of those plans.

3. In considering the proposal to embed BCM with wider resilience issues, LG noted that the majority of incidents which require a BC response are not security issues. This is acknowledged in the earlier paper (para 19). BCM is, however, a key factor in an organisation's resilience and there is a clear benefit from combining it with strategic consideration of wider resilience matters. On a practical level, it is likely that many of the same people would be asked to contribute to BC strategy and resilience strategy, so combining the two will result in efficiency savings.

Membership

4. While noting the diversity in grades in the proposed membership, LG questioned the lack of balance in relation to gender. There are a number of options that could be adopted in order to address this, including any one or combination of the following:

- Adding a member from the parliamentary business side of the organisation. A better gender balance could be achieved by adding either of the clerking Group Heads. Alternatively, if LG was keen to continue to make appointments from outwith LG, several senior clerking positions – including in the Parliamentary Business Team – are currently held by women;
- Adding a member from outwith the directly engaged teams. This could be provided to someone seen as a future leader and could act as a career development opportunity by giving a corporate role to someone identified as having potential to work beyond her current role. Seeking a gender-specific appointment would be fully justified as part of our stated aim to see gender

balance on our internal boards as part of our commitment to both the 50/50 by 2020 agenda and our wider diversity strategy;

- Removing the Head of Finance and Security from formal board membership. LG questioned the need for both this post holder and the Head of Security to sit on the Board due to the overlap in their areas of responsibility. The former was proposed for membership not only for his overall responsibility for security matters, but due to the fact that much of the Member-facing response to security is managed through the Members' Expenses Scheme and that responding to the recent Police Scotland review of physical security will require decisions on financial investments. The Board could, however, seek advice from the Head of Finance and Security on an ad hoc basis, should LG be attracted to this option.

5. No further changes to the membership proposed at para 21 are proposed. Adopting all three proposals above would result in a composition of 4 male and 3 female members, with the external appointee to be added.

Resource Implications

6. There are no additional resources required for the establishment of the Resilience Board. Operational responsibility for physical, personnel and cyber security will continue to lie with the Security Office and BIT respectively and will continue to be managed within existing budgetary arrangements. The BC Manager holds a budget for business continuity matters and will report to the Resilience Board on the management of that budget.

Dependencies

7. There are no specific dependencies relating to the establishment of the board beyond the agreement of LG. Once established, the successful management of the board depends on its members and the appropriate involvement of external partners.

Governance issues

8. The Board will be chaired by an Assistant Chief Executive and is accountable to LG for its actions.

Publication Scheme

9. This paper can be published.

Next steps

10. Should LG agree to this proposal, the Board will be established immediately and a representative of the CPNI invited to join.

Decision

11. Leadership Group is asked to agree to the establishment of a Resilience Board on the lines set out in the paper and in LG Paper 075 attached in Annex A.

**David McGill
October 2017**

RESILIENCE BOARD

Executive summary

12. This paper proposes the establishment of a Board to provide strategic direction on all matters governing the Parliament's preparation for and recovery from disruptive incidents. This will focus on personnel, physical and cyber security at the Parliament and will include all business continuity work in order to bring together the Parliament's planning and response to significant incidents.

Issues and Options

13. The Parliament's Strategic Plan lists as one of its priorities "*safe, secure and resilient working environments for Members, Members' staff, the Scottish Parliamentary Service and the Public*". The Delivery Plan commits us to "*establish a mechanism for instigating and overseeing a strategic approach to physical and cyber security*". In addition to these commitments, there is a number of actions relating to security and cyber security in the Delivery Plan that are either under consideration or require to be addressed.

14. Recent events have added to the focus on security matters at Holyrood. An external review of security conducted by Police Scotland earlier this year resulted in a detailed report containing 95 recommendations for changes to both improve security of the campus and the safety of those who use the building being presented to the SPCB. Consideration of the recommendations which might improve physical security measures in the building involves analysis of projected benefits, costs of implementation and impact on the Parliament's accessibility. This will require significant input from Security Office staff and will include regular communication with the SPCB and with Police Scotland before decisions are taken on all but the most straightforward recommendations.

15. LG has been well briefed on the recent brute-force cyber-attack on the Parliament's IT systems. The unprecedented attack began on 15 August and lasted several weeks. Although the Parliament's defences stood up well to the attack and a potentially damaging data breach was avoided, several lessons on preparing for and responding to such attacks were learned. At a strategic level, the respective roles of security partners such as the National Cyber Security Centre and Police Scotland as well as the needs and expectations of major stakeholders such as MSPs and the Scottish Government were factors to which our response was necessarily reactive. Resisting the attack was, obviously, the clear priority but time now requires to be taken to address these issues in advance of any similar attacks which may, according to security experts, be all but inevitable.

16. Considering the breadth of issues affecting the security of the Parliament, it is proposed to establish a board to provide strategic direction on all aspects of the Parliament's security functions and requirements. Due partly to the close relationship between security incidents and business continuity responses to such incidents and the need to avoid a cluttered corporate governance landscape, it is further proposed that strategic support for business continuity matters is added to the remit of the new board. The current Business Continuity Board will, as a consequence be disbanded with operational matters covered as follows.

Business Continuity

17. Business Continuity has evolved considerably over recent years. From a very centralised model, BC is now managed on a devolved model which places responsibility for maintaining and testing plans at the local level. The BC Manager supports business areas in this responsibility and reports to a corporate-level BC Board. Much of the recent focus of BC planning has been on security issues including improving the Parliament's preparedness for a CBRN (chemical, biological, radiological, nuclear) attack and collaborating with the Security Office on developing plans to respond to a Marauding Terrorist Firearms Attack (MTFA), both of which have grown in prominence globally in recent years. While it is by no means the case that all BC planning relates to security issues, it is clear that there are strong connections and that there is considerable merit in incorporating BC considerations into strategic security issues.

18. To assist with the implementation of the business continuity programme, a cross-cutting and more tactically focused group will provide advice to, and take action from the board on issues specifically focused on business continuity, whether those arise from the security maturity programme or elsewhere. This group will help ensure there is a consistent approach to business continuity planning for our essential activities and will lead on the development of the Parliament's Incident Management planning arrangements including the review and development of our overall approach, improving/reporting on the arrangements in place and ensuring the plan is exercised.

Remit

19. Taking account of the above, the following remit for the new board is suggested:

To provide strategic direction on the Parliament's preparations for and recovery from significant incidents, with a focus on personnel, physical and cyber security.

It is further proposed that the significant incidents referred to in the draft remit includes the Parliament's role in Operation London Bridge and, specifically, in Operation Unicorn.

Membership

20. The following Membership of the Resilience Board is proposed:

David McGill (Chair)
Alan Balharrie
Becky Thomson
Tommy Lynch
Derek Croll
Huw Williams

In addition, it is proposed that an appropriate external presence is added to provided wider expertise and links into relevant partners. Three main options to provide this

contribution are Police Scotland, the NCSC and the Centre for the Protection of the National Infrastructure (CPNI).

21. Police Scotland and the NCSC both have relatively specific roles and while both are likely to be very important partners in improving our management of security issues, the Resilience Board requires a wider perspective on security issues. The CPNI, which sits within MI5, has a strong advisory role in relation to security matters. It operates in line with national policies such as the National Security Strategy, National Risk Register and the Counter Terrorism Strategy. As such, it has links to all aspects of security planning and response and is therefore considered the best fit for strategic advice to the Resilience Board. The CPNI adviser that currently works with the Parliament also supports the Scottish Government and the National Assembly for Wales and therefore has a good understanding of the Scottish context and working in political environments.

Resource Implications

22. There are no additional resources required for the establishment of the Resilience Board. Operational responsibility for physical, personnel and cyber security will continue to lie with the Security Office and BIT respectively and will continue to be managed within existing budgetary arrangements. The BC Manager holds a budget for business continuity matters and will report to the Resilience Board on the management of that budget.

Dependencies

23. There are no specific dependencies relating to the establishment of the board beyond the agreement of LG. Once established, the successful management of the board depends on its members and the appropriate involvement of external partners.

Governance issues

24. The board will be chaired by an Assistant Chief Executive and is accountable to LG for its actions.

Publication Scheme

25. This paper can be published.

Next steps

26. Should LG agree to this proposal, the board will be established immediately and a representative of the CPNI invited to join.

Decision

27. LG is asked to agree to the establishment of a Resilience Board with the remit and membership set out above, with consequential changes to the management of business continuity matters.

David McGill
September 2017